РОССИЙСКОЕ АГЕНТСТВО ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ
(РОСПАТЕНТ)

ФЕДЕРАЛЬНЫЙ ИНСТИТУТ ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ

рег.No 20/12-890 "28"ноября 2001 г.

С П Р А В К А

Федеральный институт промышленной собственности Российского агентства по патентам и товарным знакам настоящим удостоверяет, что приложенные материалы являются точным воспроизведением первоначального описания, формулы и чертежей (если имеются) заявки на выдачу патента на изобретение № 2000133391, поданной в декабре месяце 29 дня 2000 года (29.12.2000).

Название изобретения	Вычислительная сеть с межсетевым экраном и межсетевой экран
Заявитель	КУПРЕЕНКО Сергей Витальевич ЗАБОРОВСКИЙ Владимир Сергеевич ШЕМАНИН Юрий Алексеевич
Действительный автор(ы)	КУПРЕЕНКО Сергей Витальевич ЗАБОРОВСКИЙ Владимир Сергеевич ШЕМАНИН Юрий Алексеевич

CERTIFIED COPY OF PRIORITY DOCUMENT

Заместитель директора Института В.Ю.Джермакян

Вычислительная сеть с межсетевым экраном и межсетевой экран.

Настоящее изобретение относится к сфере обеспечения информационной безопасности и, в частности, касается аппаратно-программных компонент межсетевых экранов, используемых для предотвращения несанкционированного доступа и обмена информацией между различными абонентами компьютерных сетей.

В настоящее время большинство локальных вычислительных сетей (ЛВС) подключены к сети Интернет. Однако отсутствие встроенных средств защиты информации в существующих сетевых протоколах является причиной различных нарушений целостности передаваемых данных. Поэтому расширение спектра и повышение требований к уровню конфиденциальности сетевых приложений требует использования специальных технических средств разграничения доступа к информационным ресурсам и контроля обмена данными между различными компьютерными сетями. В качестве таких средств защиты широко применяются межсетевые экраны, называемые в англоязычной литературе фаэрволами (firewall). Межсетевой экран представляет собой специализированное сетевое устройство, которое включается между двумя сегментами ЛВС таким образом, что весь обмен сетевыми пакетами между этими сегментами ограничивается с помощью специальных правил фильтрации входящих и исходящих потоков данных. Такое устройство может быть также установлено между защищаемым сегментом ЛВС и маршрутизатором, один из

портов которого подключен к сети Интернет. При этом используемые правила фильтрации пакетного трафика могут включать запрет на передачу информации как изнутри, так и вовнутрь защищаемого сегмента ЛВС, включая контроль определенных пользователей в установленные интервалы времени суток, недель или месяцев.

Известна система защиты для двух компьютерных сетей, описанная в российской патентной заявке А 96118130/09. Эта система защиты содержит две сетевые материнские платы и предназначена для предотвращения несанкционированных обменов данных между первой и второй компьютерными сетями. Каждая из указанных плат имеет сетевой интерфейсный адаптер для обмена данными с указанными выше сетями. При этом каждая из указанных материнских плат также имеет адаптер передачи данных для обмена информации с адаптером другой сетевой материнской платы и использует специальные программные средства для предотвращения передачи информации об услугах маршрутизации между сетевыми интерфейсными адаптерами и адаптером передачи данных. Каждая сетевая материнская плата дополнительно содержит программные средства преобразования протокола, препятствующие прохождению информации о функционировании протокола верхнего уровня и информации об адресе источника и адресе назначения между указанным выше сетевым интерфейсным адаптером и указанным адаптером передачи данных каждой сетевой материнской платы. При этом одна из сетевых материнских плат имеет специальные программные средства поддержания интерфейса

взаимодействия на прикладном уровне для выполняемых соответствующих задач.

Описанная выше система защиты по выполняемым функциям может быть классифицирована как сервер-представитель (proxy-сервер) или узел компьютерной сети, устанавливающий соединения от имени и по поручению зарегистрированного сетевого клиента.

При использовании proxy-сервера в качестве межсетевого экрана требуется, чтобы сетевой клиент осуществлял ряд дополнительные сеансов связи по установлению сетевых соединений, что приводит к снижению общей сетевой производительности и увеличению задержек передачи пакетов особенно в случае последовательного соединения нескольких компьютерных сетей, разделенных между собой межсетевыми экранами указанного типа.

Эти недостатки преодолены в изобретении, раскрытом в патенте US 5,898,830, которое является наиболее близким к настоящему изобретению. Этот межсетевой экран, будучи установленным в канал информационного обмена между двумя компьютерными сетями, обеспечивает прозрачность межсетевого взаимодействия для пользователей защищенного сегмента. Для этого межсетевой экран поддерживает конфигурацию двух наборов виртуальных абонентов. Первый набор абонентов может быть адресован только со стороны защищенного, а второй - со стороны открытого сегментов сети.

Рассматриваемые наборы виртуальных абонентов программно связаны между собой с помощью таблицы соответствия их сетевых

адресов, аналогично тому, как это делается при использовании DNS серверов. Передача или запрет передачи пакетов от виртуального абонента одного набора адресов к виртуальному абоненту из другого набора адресов осуществляется в соответствии с правилами фильтрации пакетов, сохраняемыми в конфигурационном файле межсетевого экрана.

Виртуальные абоненты, за исключением одного, который специально выделен для этой цели, не имеют доступа к файловой системе и другим системным ресурсам устройства, на котором фактически реализован межсетевой экран. Управляющий программный модуль осуществляет конфигурацию межсетевого экрана, в частности, генерацию виртуальных абонентов в соответствии с записанным конфигурационными файлами при первоначальном старте данного устройства. Доступ к конфигурационным файлам осуществляется с использованием правил с функциями авторизации через специального виртуального абонента, адресуемого из компьютерной сети. Эти правила включают проверку подлинности и авторизацию запрашивающего доступ абонента. Когда доступ запрашивающему абоненту предоставлен, в конфигурационный файл межсетевого экрана, контролирующего информационный обмен между компьютерными сетями, могут быть внесены изменения.

Упомянутая выше прозрачность экрана по отношению к протоколам сетевого уровня не означает, что экран не может быть обнаружен при применении специальных программных средств. Так как набор защищаемых сетевых узлов экранируется одним

сетевым интерфейсом рассматриваемого устройства защиты, то на канальном уровне межсетевого взаимодействия каждый из этих узлов идентифицируется по соответствующему физическому адресу этого же сетевого интерфейса.

Процедура проверки подлинности абонента сети, уполномоченного на получение доступа к конфигурационному файлу, уязвима для злоумышленников, что подразумевает возможность несанкционированного доступа вследствие подбора паролей или использования не выявленного несовершенства программного обеспечения применяемого устройства защиты.

В основу настоящего изобретения положен принцип гарантированной безопасности, основанный на неиспользовании или полном сокрытии адресов сетевых интерфейсов устройства защиты.

Поставленная задача решается тем, что межсетевой экран, обладая сетевыми интерфейсами для обмена данными между сегментами сети, рассматривается как не адресуемый (пассивный) сетевой узел, то есть не использует при своем функционировании сетевых адресов, ассоциируемых с этими интерфейсами обмена, а физические адреса сетевых интерфейсов не передает во внешнюю сеть.. Поэтому наличие межсетевого экрана не может быть обнаружено никакими техническими средствами, расположенными в открытом или защищенном сегменте сети. Согласно изобретению, для управления процессами фильтрации пакетного трафика межсетевой экран дополнительно содержит, изолированный от сетевых интерфейсов, специальный интерфейс управления. Все

изменения программы фильтрации пакетного трафика, а также управление сетевыми соединениями могут быть выполнены исключительно через интерфейс управления, что полностью устраняет возможность несанкционированного доступа к межсетевому экрану со стороны пользователей расположенных как в защищенном, так и в открытом сегментах ЛВС. Задача обеспечения гарантированной защиты решается также с помощью невозможности создания со стороны пользователей открытого и/или защищенного сегментов сети специального канала передачи пакетных данных между сетевыми интерфейсами и управляющим интерфейсом с помощью внутренней системной шины вычислителя, на базе которого построен межсетевой экран. При этом межсетевой экран сохраняет неизменной информацию об адресах отправителя и/или получателя обрабатываемого с помощью правил фильтрации пакетов, что позволяет полностью скрыть факт существования межсетевого экрана для пользователей защищенного сегмента сети.

Иными словами, программа фильтрации исключает межсетевой экран из числа получателей информационных пакетов, поступающих на сетевые интерфейсы, а межсетевой экран настроен передавать вовне через сетевые интерфейсы, исключительно такие информационные пакеты, отправители которых являются внешними по отношению к межсетевому экрану.

Настоящее изобретение подробно рассмотрено далее на примере его реализации со ссылками на чертежи, на которых:

Фиг. 1 изображает внешний вид выполненного согласно настоящему изобретению межсетевого экрана, со стороны панели, на которой расположены органы управления и интерфейсы внешних соединений;

Фиг. 2 - схему соединения двух локальных вычислительных сетей между собой и с внешней сетью через межсетевой экран, выполненный согласно настоящему изобретению.

Фиг. 3 - упрощенный алгоритм программы управления передачей информационных блоков, поступающих на один из интерфейсов обмена межсетевого экрана, выполненного согласно настоящему изобретению.

Описание, приведенное ниже, предполагает знакомство с наиболее употребительными терминами и понятиями, относящимися к вычислительной технике, и в частности, к вычислительным сетям.

В соответствии с предпочтительной реализацией настоящего изобретения, изображенный на Фиг. 1 межсетевой экран 1, приспособленный для работы в локальной вычислительной сети (ЛВС), представляет собой специализированный вычислитель со встроенной операционной системой. Такой вычислитель может быть выполнен с использованием серийно выпускаемых материнских плат персональных компьютеров, например, платы фирмы Gygabyte, GA-5AX, в которой предусмотрена возможность подключения до 5-ти периферийных устройств к внутренней системной шине PCI. Вычислитель межсетевого экрана, на котором выполняются задачи фильтрации под управлением встраиваемой операционной системы

может быть выполнен на базе нескольких типов процессоров общего назначения, включая Pentium MMX, Cyrix MII, AMD K-6, RISC MIPS и др. Межсетевой экран 1 содержит сетевые интерфейсы для обмена пакетными данными, в качестве которых могут быть использованы сетевые адаптеры Ethernet различного типа со скоростью передачи 10 Мбит/с для шины ISA или 10/100 Мбит/с для шины PCI, например, Fast Etherlink XL фирмы 3Com. На лицевой панели 2 межсетевого экрана 1 расположены соединители для трех интерфейсов обмена данными, обозначенных позициями 3, 4, 5. К каждому из сетевых адаптеров подключен сегмент локальной вычислительной сети, построенной по архитектуре общей шины и использующей протокол Ethernet. Межсетевой экран 1 может быть приспособлен для подключения большего количества сегментов ЛВС, в частности, используемая материнская плата может обеспечить подключение до 5-ти сегментов ЛВС. Если в ЛВС используется другой протокол, то применяемые сетевые адаптеры межсетевого экрана, должны поддерживать этот протокол взаимодействия.

На панели 2 установлены также соединители на 9 и 25 контактов, соответственно, интерфейсов 6 и 7 COM портов стандарта RS232C. Один из них используется в качестве интерфейса управления для редактирования программы управления информационным обменом между сетевыми сегментами ЛВС, соединяемыми через межсетевой экран 1. Сегменты ЛВС, в зависимости от их количества, могут быть подключены к

интерфейсам 3, 4, или 3, 4, 5, соответственно. На панели 2 установлен также соединитель 8 и выключатель 9 электропитания.

В рассматриваемом примере реализации изобретения, в межсетевом экране 1 используется операционная система типа UNIX, обеспечивающая многозадачную работу программы управления в соответствии с конфигурационным файлом, сохраняемым в энергонезависимом устройстве памяти межсетевого экрана 1.

Фиг. 2 иллюстрирует один из вариантов подключения ЛВС к межсетевому экрану 1. В этом примере межсетевой экран 1 делит защищаемую корпоративную ЛВС 10 с шинной архитектурой на сегменты 11, 12, 13 подключенные, соответственно, к сетевым адаптерам 3, 4, 5. Такая структура ЛВС 10 может использоваться в корпоративной компьютерной сети, в которой разные сетевые сегменты предназначены для обслуживания разных типов информационных приложений. Эти приложения могут иметь различные требования к уровню конфиденциальности передаваемых данных, что учитывается в правилах фильтрации, применяемых для каждого из сетевых интерфейсов.

В настоящем примере сегмент 13 содержит только одного абонента, шлюз 14, который обеспечивает соединение ЛВС 10 с внешней сетью 15. Сеть 15, в свою очередь, может быть соединена с другими сетями. Шлюз 14 может использовать модемные линии связи для соединения ЛВС 10 с сетью Интернет по коммутируемым каналам.

Каждый из сегментов 11, 12 ЛВС содержит несколько абонентов 16, 17, соответственно, подключенных к этим сетевым

сегментам с помощью адаптеров 18 типа Ethernet. Для внесения изменений в программу управления передачей сетевых пакетов между интерфейсами 3, 4 и 5, которые могут касаться правил фильтрации, к управляющему интерфейсу 6 подключают персональный компьютер 19. Редактирование программы управления осуществляется на компьютере 19 с помощью стандартной программы Web навигатора (браузера), например, Netscape Navigator путем установления авторизованного с помощью пароля соединения между компьютером 19 и межсетевым экраном 1 по протоколу «точка - точка» (протокол PPP).

Программа управления обеспечивает передачу сетевых пакетов между сетевыми интерфейсами, которые адресованы к пользователям открытого или защищенных сегментов. Так как межсетевой экран не имеет адресов, ассоциируемых с его сетевыми интерфейсами, то он не может являться получателем никаких сетевых пакетов, а выступает в роли либо пассивного транзитного узла между сетевыми интерфейсами, либо моделирует разрыв сетевого соединения путем отбрасывания пакетов, не прошедших, установленные для пути между данными интерфейсами, правила фильтрации.

Программа управления, которая контролирует работу интерфейсов 3, 4, 5 обмена пакетными данными (драйвер сетевых адаптеров Ethernet) настроена таким образом, что содержимое поля адреса отправителя в информационных блоках, передаваемых из межсетевого экрана 1 через интерфейсы 3, 4, 5, сохраняется неизменным.

Шлюз 14 выполняет функции маршрутизатора, обменивающегося информацией о состоянии сетевых соединений с аналогичными устройствами и передающего пакетный трафик в другие сегменты корпоративной сети или сеть Интернет.

Таким образом, ЛВС 10 может быть надежно защищена межсетевым экраном, сетевые интерфейсы которого, согласно настоящему изобретению, не имеют как физических (MAC), так и логических (IP) адресов. Такой межсетевой экран недоступен для удаленных атак через компьютерные сети, так как не может являться получателем информационных пакетов. Еще раз подчеркнем, что межсетевой экран не может быть обнаружен стандартными средствами сетевой идентификации, так как используемые для связи с сетевыми сегментами интерфейсы типа Ethernet управляются таким образом, что не отвечает на широковещательные ARP запросы о своем физическом (MAC) адресе.

Фиг. 3 иллюстрирует работу алгоритма фильтрации пакетов, поступающих на сетевой интерфейс 5.

Каждый пакет, передаваемый через сегмент 11 в ЛВС 10, принимается интерфейсом 5 и заносится в буферную память. Первичная обработка согласно правилам фильтрации состоит в последовательном выполнении операций 20, 21, то есть последовательной проверке принадлежности физического адреса Ad получателя, содержащегося в заголовке обрабатываемого пакета, занесенному в таблицу К3 списку разрешенных адресов для абонентов сегмента 11 (Фиг. 2), подключенного к интерфейсу 3,

а затем к списку адресов абонентов подключенного к интерфейсу 4 сегмента 12, содержащемуся в таблице К4.

Пакет с адресом получателя, который отсутствует в обеих таблицах К3, К4 - отбрасывается. Если адрес получателя принадлежит таблице К3, то производится проверка пакета в соответствии с набором правил Тест 3, изображенная операцией 22, в противном случае используется операция 23 содержащая другой набор правил, Тест 4.

Возможность использования различных правил проверки информационных блоков, адресованных в разные сегменты ЛВС 10, позволяет разделить абонентов по уровню безопасности и категориям приложений. В соответствии с этими категориями различные пользователи подключаются к разным сетевым сегментам, например, к сегменту базы данных авторизированных пользователей или сегменту технического отдела корпоративной сети. Правила фильтрации пакетов устанавливаются и изменяются только администратором ЛВС 10 с помощью компьютера 19, который по специальному каналу с использованием пароля доступа через выделенный управляющий интерфейс 6 (Фиг.2) на определенное время, необходимое для внесения изменений, подключается к межсетевому экрану.

Результаты проверки по наборам правил Тест 3 и Тест 4 ассоциируются с логическими переменные Т3 и Т4, принимающие значение TRUE, если передача информационного блока разрешена, операции 24, 25. Если Т3 = TRUE, то пакет передается через интерфейс 3 в сегмент 11. Если пакет, адресованный в сегмент

12, успешно прошел проверку по набору правил Тест 4, то переменная T4 = TRUE, и пакет передается через интерфейс 4. При несоответствии требованиям правил фильтрации пакет отбрасывается.

Обработка пакета в межсетевом экране 1, поступающих, например, через интерфейс 3, производится в соответствии с описанным выше алгоритмом (Фиг. 3) за исключением применения тех правил, которые используются для защиты направления передачи «интерфейс 3 – интерфейс 5» или «интерфейс 3 – интерфейс 4».

Описанный выше характер функционирования межсетевого экрана не исчерпывает очевидных специалисту вариантов применения настоящего изобретения не выходящих за пределы существа предложенного решения, которые определяются формулой изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Локальная вычислительная сеть передачи пакетов, в заголовках которых содержатся сведения о физических и логических адресах отправителя и/или получателя информации, имеет разделяющий ее по меньшей мере на два сегмента межсетевой экран, представляющий собой комплекс аппаратных и программных средств, содержащий по меньшей мере два сетевых интерфейса для обмена двунаправленными потоками пакетов между сегментами сети и программу управления процессами пакетной коммутации между сетевыми интерфейсами, которые происходят на основе применения правил фильтрации, отличающаяся тем, что программа управления не назначает сетевым интерфейсам логических адресов и не передает в вычислительную сеть информацию об их физических адресах, при этом программа управления разрешает транзитную передачу через сетевые интерфейсы межсетевого экрана только тех пакетов, параметры заголовков которых прошли проверку на соответствие установленным правилам фильтрации, а для задания этих правил и контроля за состоянием сетевых соединений используется отдельный, не имеющий связи с сетевыми интерфейсами, интерфейс управления.

2. Вычислительная сеть по п. 1, отличающаяся тем, что при прохождении пакетов через сетевые интерфейсы в их заголовках сохраняется без изменения информация о физическом адресе отправителя пакета, так как программа управления межсетевым экраном не передает во внешнюю сеть информацию о физических

адресах своих сетевых интерфейсов.

3. Вычислительная сеть по п. 1, отличающаяся тем, что межсетевой экран построен на базе универсального вычислителя со встроенной операционной системой, а также нескольких сетевых интерфейсов и выделенного управляющего интерфейса, причем сетевые интерфейсы являются адаптерами типа Ethernet, а интерфейс управления может быть выполнен как на базе интерфейса типа Ethernet, так и на базе последовательного асинхронного интерфейса.

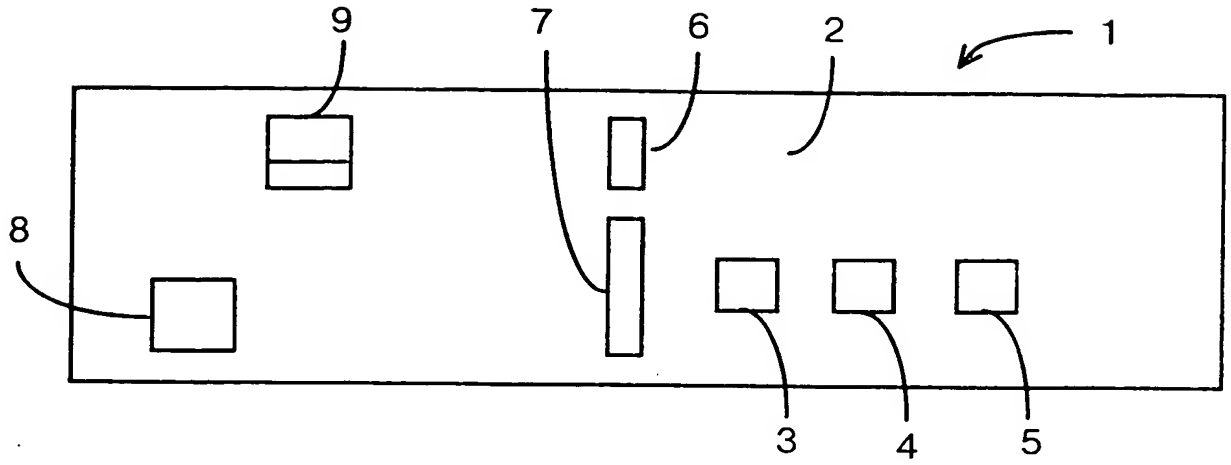
4. Вычислительная сеть по п. 1, отличающаяся тем, что правила фильтрации, выполняемые межсетевым экраном, запрещают транзитную передачу любых пакетов между сетевыми интерфейсами, кроме тех, которые имеют разрешенные признаки и параметры адресации в своих заголовках.

5. Вычислительная сеть по п. 1, отличающаяся тем, что доступ к программе редактирования правил фильтрации межсетевого экрана защищен паролем.

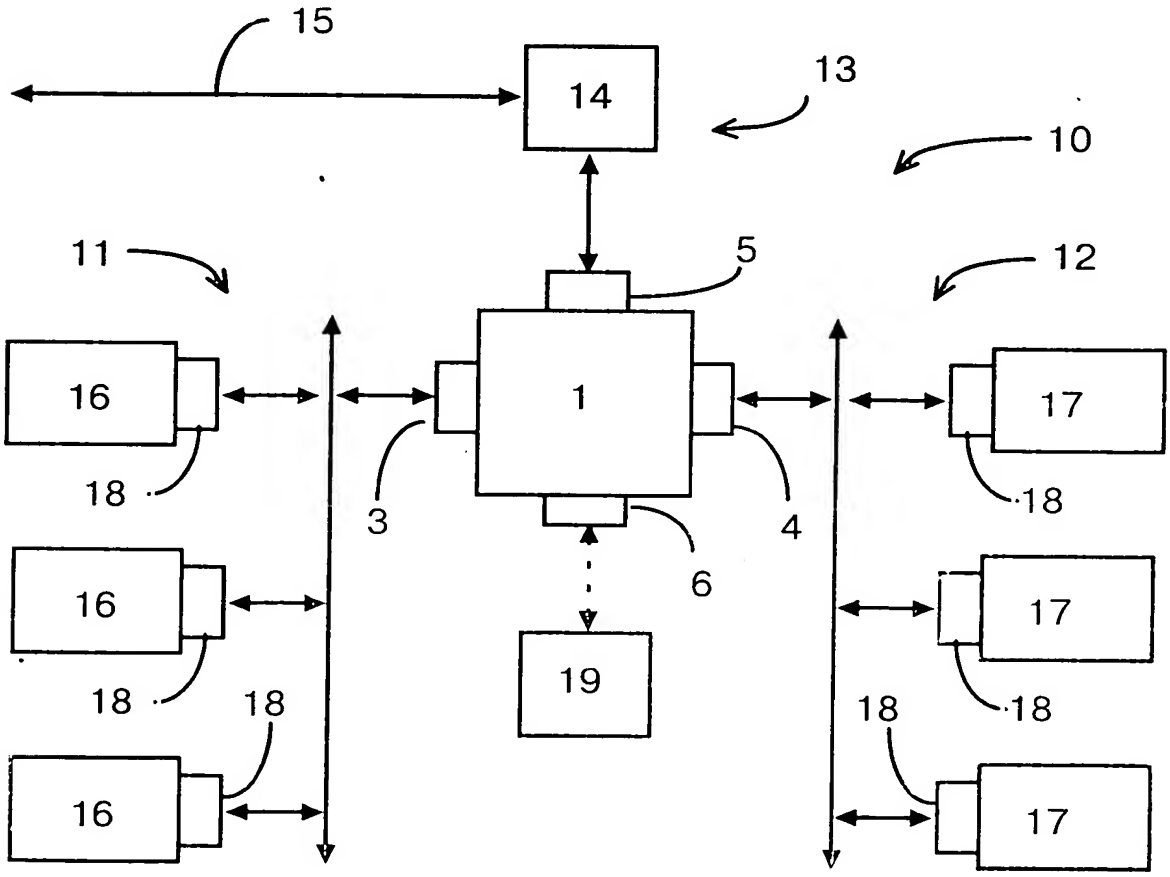
6. Межсетевой экран представляющий собой комплекс аппаратных и программных средств, содержащий по меньшей мере два сетевых интерфейса для пакетной коммутации данных между сегментами вычислительной сети, а также программу управления передачей пакетов между сетевыми интерфейсами в соответствии с правилами фильтрации, отличающийся тем, что после обработки пакета в соответствии с правилами фильтрации сохраняет без изменений информацию о физическом и логическом адресах отправителя каждого из пакетов, содержащуюся в их заголовках,

причем программа управления не назначает сетевым интерфейсам логических адресов и не передает в связанные с ними сетевые сегменты информацию об их физических адресах, межсетевой экран содержит специальный интерфейс управления для редактирования, контроля и настройки правил фильтрации, причем любые изменения параметров фильтрации могут осуществляться исключительно через интерфейс управления, при этом программа управления обеспечивает передачу пакета с одного сетевого интерфейса на другой на основании информации, содержащейся в заголовке пакета, только в тех случаях, когда адреса получателей и/или отправителей пакетов удовлетворяют всем требованиям, определенным в правилах фильтрации пакетов.

7. Межсетевой экран по п. 6, отличающийся тем, что построен на базе вычислителя со встроенной операционной системой, универсальной шиной обмена данными между интерфейсными адаптерами и выделенным каналом управления, доступ к которому защищен паролем.

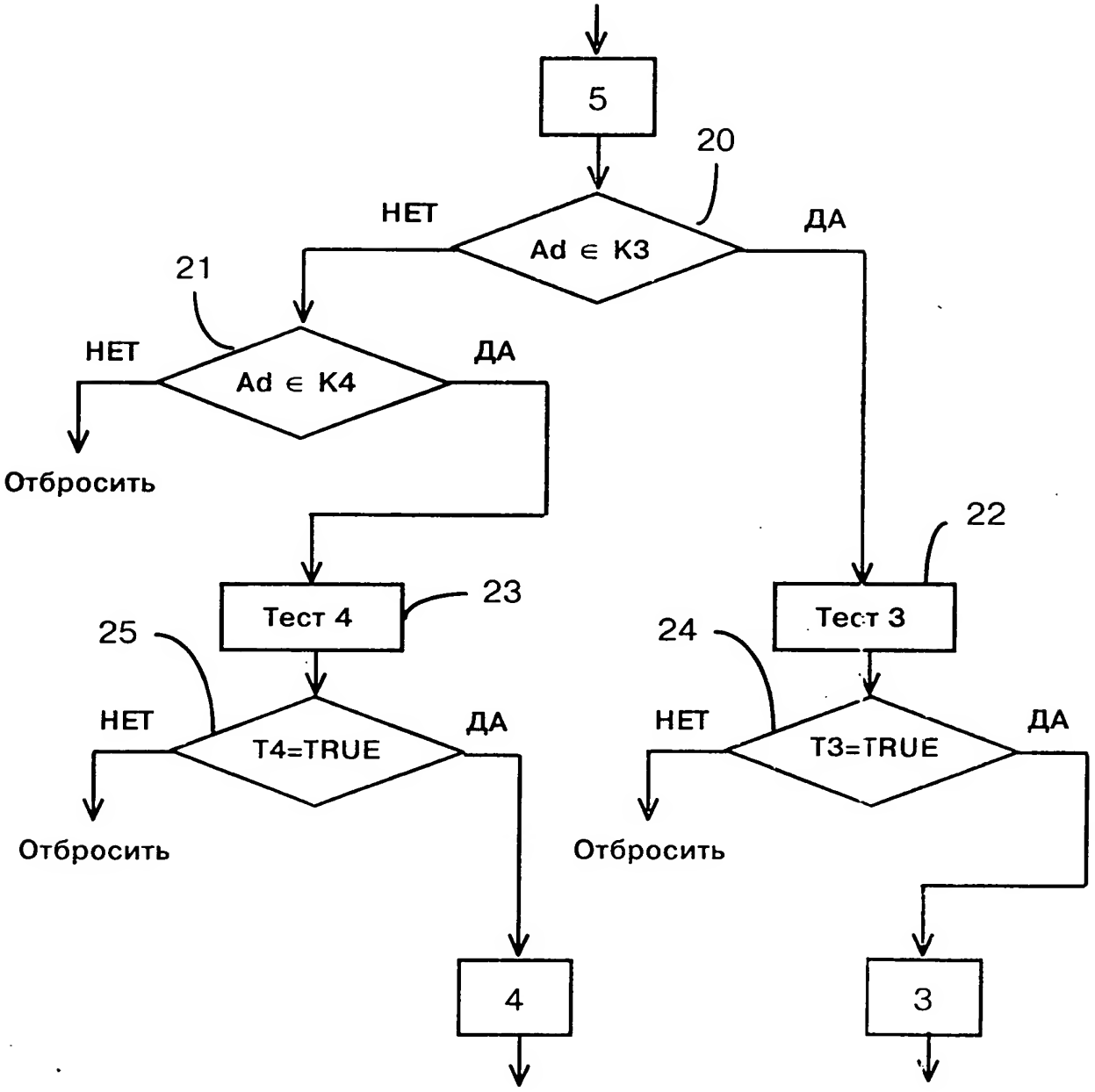

9
7
6
2
1
8
3
4
5

Фиг. 1


15
14
13
10
11
5
12
16
1
17
18
3
4
18
6
16
17
19
18
18
18
16
17

Фиг. 2

Вычислительная сеть с межсетевым экраном и межсетевой экран.



Фиг. 3

Вычислительная сеть с межсетевым экраном и межсетевой экран.

РЕФЕРАТ

Межсетевой экран для локальных вычислительных сетей содержит по меньшей мере два сетевых интерфейса для пакетной коммутации данных между сегментами вычислительной сети, выполняемой в соответствии с программой фильтрации пакетов. Межсетевой экран после обработки пакета в соответствии с правилами фильтрации сохраняет без изменений информацию о физическом и логическом адресах отправителя каждого из пакетов, содержащуюся в их заголовках. Программа управления не назначает сетевым интерфейсам логических адресов и не передает в связанные с ними сетевые сегменты информацию об их физических адресах. Чтобы обеспечить внесение изменений в правила фильтрации межсетевой экран содержит специальный интерфейс управления, причем любые изменения параметров фильтрации могут осуществляться исключительно через интерфейс управления.

2 н. п. ф-лы, Фиг. 2.